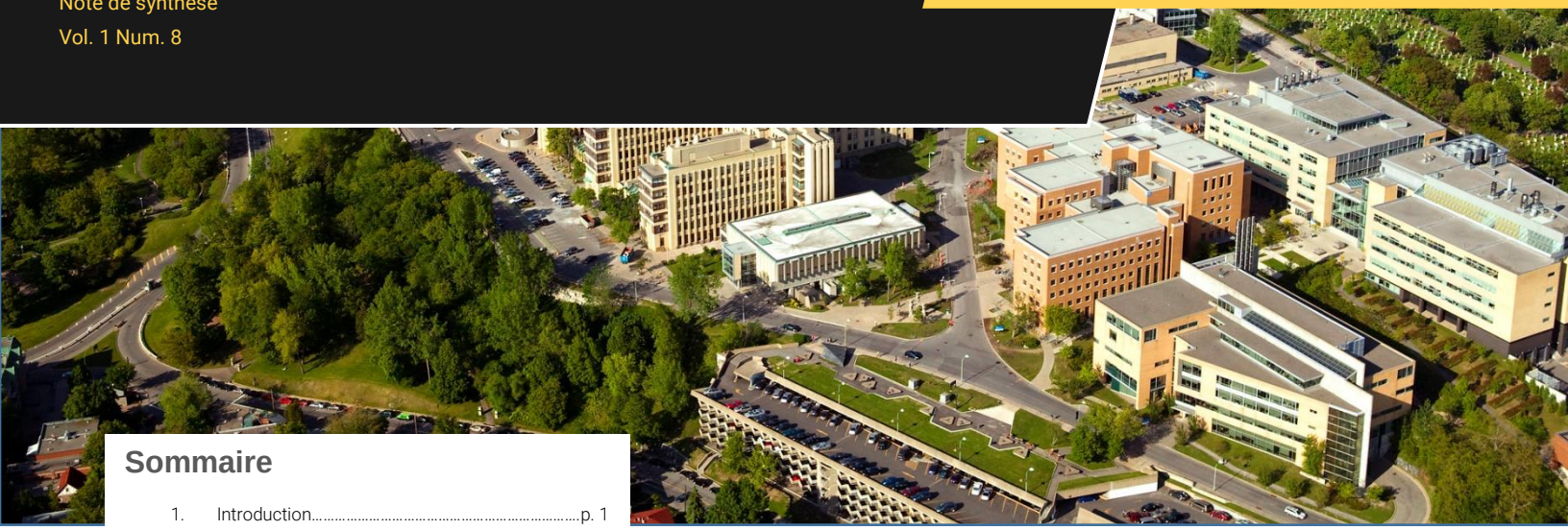
Les campagnes de prévention en cybersécurité

Cameron Coutu, M. Sc.

Note de synthèse
Vol. 1 Num. 8

CRPC | Chaire de recherche en prévention de la cybercriminalité



Sommaire

Coutu, C. (2019). La prévention de la cybercriminalité : résultats d'une enquête sur les effets perçus d'une campagne de prévention réalisée par une institution financière (mémoire de maitrise, Université de Montréal).

La Chaire de recherche en prévention de la cybercriminalité a été créée à l'initiative de l'Université de Montréal, de Desjardins et de la Banque Nationale du Canada. Dirigée par Benoît Dupont, chercheur au Centre international de criminologie comparée de l'Université de Montréal, elle a pour mission de contribuer à l'avancement de la recherche sur les phénomènes cybercriminels sous l'angle de leur prévention.

Introduction

Les campagnes de prévention sont habituellement utilisées en santé publique afin de promouvoir de saines habitudes de vie. En criminologie, les campagnes de prévention peuvent participer à la protection du public à travers des stratégies d'information communiquées à la population quant aux risques encourus et afin d'inciter l'adoption de comportements sécuritaires.

Ces dernières années, les gouvernements, ainsi que certaines grandes institutions financières, ont élaboré des campagnes visant à sensibiliser la population ou la clientèle desservie sur les moyens à prendre pour se protéger contre la cybercriminalité.

Cette note de synthèse vise à présenter sommairement les approches ou modèles théoriques ayant guidé le développement de stratégies préventives en cybersécurité. Des recommandations en lien avec le développement de nouvelles stratégies de prévention seront également présentées.

La prévention du crime

En criminologie, la prévention du crime fait référence à tout moyen ou stratégie visant à réduire la sévérité et la fréquence des infractions criminelles[1].

La prévention du crime peut être classée selon trois niveaux : primaire, secondaire et tertiaire[2 3].

- La prévention primaire est dirigée vers la modification des conditions qui, dans l'environnement physique et social, peuvent mener au crime.

- La prévention secondaire cible des personnes et des groupes à risque d'être incriminés ou victimisés. Elle repose sur un dépistage précoce, suivi d'interventions sur les individus considérés à risque d'être impliqués dans un crime.

- La prévention tertiaire se concentre sur les effets observés après qu'un crime a été commis. Son but principal est la réduction de la récidive. Les campagnes de prévention à ce niveau se concentrent sur la détection, la condamnation, la punition ou le traitement correctionnel des personnes contrevenantes.

Quelques modèles théoriques de la prévention adaptés à la cybercriminalité

La prévention de la cybercriminalité s'inspire souvent de modèles théoriques provenant d'autres domaines, notamment la santé publique. Avec ce type d'approche, l'intervention n'est plus axée sur le délinquant ou l'environnement physique mais plutôt sur les victimes potentielles en les encourageant à être proactives en prenant les précautions nécessaires pour se protéger.

Les modèles théoriques suivants semblent être les mieux adaptés à la prévention de la cybercriminalité:

- Protection Motivation Theory (PMT) : cette théorie suggère que l'adoption de mesures de protection par un individu dépend de sa perception de la menace (sévérité perçue et susceptibilité perçue) et de sa capacité à s'y adapter et à y faire face (efficacité de la réponse et auto-efficacité). Ces deux processus cognitifs seraient stimulés en présence d'une menace, ce qui déclencherait des comportements protecteurs dans le but d'en réduire les effets[4].

- Health Belief Model (HBM) : le HBM permet de comprendre les processus cognitifs (croyances, biais et représentations) qui agissent dans l'adoption de comportements sécuritaires. Ce modèle théorique stipule qu'il existe deux déterminants basés sur les croyances des individus: 1) les perceptions de menaces et 2) les attentes perçues par rapport à l'efficacité du comportement à adopter[5 6].

Ainsi donc, une piste prometteuse consiste à mieux documenter les attitudes et les représentations des usagers afin de comprendre leurs croyances en ce qui concerne la sécurité informatique et les moyens mis à leur disposition pour garantir celle-ci.

Efficacité des campagnes de prévention

Les recherches ont démontré qu'il y a lieu de mieux cibler les efforts de prévention de la cybercriminalité. Or, les mesures de prévention et de sensibilisation du public sont relativement peu nombreuses, et celles qui existent ont rarement fait l'objet d'une évaluation. Par ailleurs, les résultats des rares évaluations disponibles se sont révélés peu fructueux[3 7].

Certaines mesures de prévention ne sont pas suffisamment arrimées aux besoins des usagers et à leur niveau de compréhension ou d'évaluation des risques encourus. Par exemple, les campagnes

de sensibilisation sur le piratage du contenu en ligne (films, jeux vidéo, etc.) ont contribué à une baisse du piratage, mais seulement sur une courte durée[8].

Les recherches évaluatives des campagnes de prévention tant en criminologie qu'en santé publique ont démontré qu'elles sont plus efficaces quand elles ciblent adéquatement les besoins du public cible et qu'elles transmettent un message clair qui favorise une réelle prise de conscience. Rares sont les mesures préventives qui prennent en considération le point de vue des usagers (leurs perceptions, leurs croyances) ou leurs connaissances des moyens à leur disposition pour se protéger.

Certaines études ont montré que les campagnes de prévention universelle (tous domaines confondus) donnent parfois des résultats positifs pour le public ciblé lorsque certaines conditions sont présentes. Ces études révèlent qu'un ingrédient clés du succès de ces campagnes est l'instauration d'une phase de maintien ou de rappel à moyen et à plus long terme.

Le problème majeur des campagnes de prévention est que les décideurs/concepteurs tentent de rejoindre le plus d'individus possible et, de ce fait, utilisent des messages trop diffus ou des généralisations ; ce qui aurait alors pour effet de diminuer l'efficacité du message transmis. Il est donc nécessaire de repenser les campagnes de manière à ce que les messages transmis portent davantage sur des objectifs plus réalistes et mieux ciblés, en proposant au public des attitudes et des comportements plus spécifiques que généraux[9].

Exemples de campagnes de prévention nationales

Depuis la dernière décennie, des gouvernements ont commencé à mettre en place des campagnes de prévention de la cybercriminalité dont en voici quelques exemples:

- En 2010, dans le cadre de la Stratégie nationale de cybersécurité, le Gouvernement fédéral canadien a lancé l'initiative « Pensez cybersécurité » [10]. À ce jour, cette stratégie a ciblé différentes problématiques en lien avec l'utilisation d'Internet telles que la cyberintimidation, la sécurité des réseaux Wi-Fi, l'importance des sauvegardes, la protection des données personnelles et la protection contre les fraudes[11].
- Les États-Unis ont aussi développé leur propre campagne nationale de prévention de la cybercriminalité nommée « Stop. Think. Connect »[12], le but étant de sensibiliser la population aux risques potentiels de l'utilisation d'Internet. Cette campagne, similaire à celle du Canada, vise aussi à informer le public des moyens à leur disposition pour se protéger et à encourager l'adoption de comportements sécuritaires en ligne.

- En Australie, le gouvernement a lancé la campagne Scamwatch sous la direction de l'Australian Competition and Consumer Commission (ACCC). La campagne de prévention met l'emphase sur les divers types de fraudes tels que les faux organismes de charité, les organismes frauduleux d'investissements, etc. Une liste de ressource est mise à disposition du public sur un site web où il est également possible d'y effectuer des signalements de cas de fraude[13].

Pistes d'amélioration pour guider de futures campagnes:

- Améliorer la visibilité et l'intensité des messages préventifs en diversifiant les canaux de diffusion;
- Prolonger la durée des campagnes pour assurer une meilleure visibilité (Par contre, il y a un risque à une trop grande visibilité : celle-ci risque en effet de provoquer ce que les experts appellent une « fatigue de sécurité » ou *security fatigue*)[14];
- Les jeux et les formations interactifs en ligne peuvent être efficaces pour augmenter l'intérêt du public ciblé[15] [16] (Voir fiche synthèse vol. 1, num. 1);
- Cibler le message en fonction de certains groupes (viser une population en particulier);
- Miser sur un thème unique (par exemple, le vol d'identité) ou sur un nombre limité de sujets pour simplifier le message préventif;
- Rendre plus explicites ou visibles les risques réels auxquels s'expose la population (en évitant de créer des peurs ou de l'anxiété) pour susciter une réelle prise de conscience (présentation de témoignages, de cas vécus).

Références

[1] Cusson, M., Dupont, B. et Lemieux, F. (2007). *Traité de sécurité intérieure*. Montréal : HMH.

[2] Monchalin, L. (2009). Pourquoi pas la prévention du crime ? Une perspective canadienne. *Criminologie*, *42*(1), 115-142.

[3] Brewer, R., De Val-Palumbo, M., Hutchings, A., Holt, T. J. , Goldsmith, A. et Maimon, D. (2019). *Cybercrime prevention:Theory and Applications*. Cham, Suisse: Palgrave.

[4] Doane, A. N., Boothe, L. G., Pearson, M. R. et Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior*, *60*, 508-513.

[5] Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs*, *2*(4), 328-335.

[6] Rosenstock, I. M., Strecher, V. J. et Becker, M. H. (1994). *The health belief model and HIV risk behavior change*. Preventing AIDS. Springer.

[7] Bada, M., Sasse, A. et Nurse, J. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118-131.

[8] Bachmann, M. (2007). Lesson spurned? Reactions of online music pirates to legal prosecutions by the RIAA. *International Journal of Cyber Criminology*, *2*, 213-227.

[9] Sacco, V. F. et Trotman, M. (1990). Public Information Programming and Family Violence: Lessons from the Mass Media Crime Prevention Experience. *Canadian J. Criminology*, *32*(1), 91-105

[10] Public Safety Canada. (2015). Canada's Cyber Security Awareness Initiative, "Get Cyber Safe".

[11] Get Cyber Safe. (2017). Campaigns.

[12] United States Department of Homeland Security. (2017). About Stop. Think. Connect.

[13] Scamwatch. (2019). Scam statistics.

[14] O'Donnell, A. (2019). Create an effective security awareness training program. *Lifeware*.

[15] Chung, H. et Zhao, X. (2004). Effects of perceived interactivity on web site preference and memory: Role *of personal motivation. Journal of Computer-Mediated Communication,* 10(1).

[16] Song, J. H. et Zinkhan, G. M. (2008). Determinants of perceived web site interactivity. *Journal of Marketing*, *72*, 99-113.